State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

June 9, 2015

ADVISORY NUMBER:
SA2015-062

DATE(S) ISSUED:
06/09/2015

SUBJECT:
Vulnerability in Windows Media Player Could Allow Remote Code Execution (MS15-057)

OVERVIEW:
A vulnerability has been discovered in Windows Media Player that could allow remote code execution. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE
There are no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:
•   **Windows Server 2003**
•   **Windows Server 2008**
•   **Windows Server 2008 R2**
•   **Windows Vista**
•   **Windows 7**

RISK:
Government:
•   **Large and medium government entities: High**
•   **Small government entities: High**
Businesses:
•   **Large and medium business entities: High**
•   **Small business entities: High**
Home users: High

TECHNICAL SUMMARY:
A vulnerability has been discovered in Windows Media Player 10,11, and 12 that could allow remote code execution due to the way Windows Media Player handles specially crafted data objects. The vulnerability could be exploited by convincing an unsuspecting user to open a specially crafted e-mail attachment or click a malicious link to an untrusted website.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RECOMMENDATIONS:
We recommend the following actions be taken:
•   Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
•   Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
•   Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
•   Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.
REFERENCES:

Microsoft:
https://technet.microsoft.com/en-us/library/security/MS15-057